Notice of Allowability	Application No.	Applicant(s)	
	10/038,295	GARSTIN ET AL.	
	Examiner	Art Unit	
	Matthew B. Smithers	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *an application filed on January 4, 2002*.

2. ☒ The allowed claim(s) is/are *1-15*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date 8/28/02; 6/13/03
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

Information Disclosure Statement

The information disclosure statements filed August 28, 2002 and June 13, 2003 have been placed in the application file and the information referred to therein has been considered as to the merits.

Allowable Subject Matter

Claims 1-15 are allowed.

The following is an examiner's statement of reasons for allowance: The present invention is a method for encrypting a packet using a stream cipher. The method eliminates the predictability of encrypted successive packets by introducing a third variable with the packet sequence number. The closest prior art, U.S. patent application 2002/0044651 granted to Tuvell, discloses a method for improving the security of cryptographic ciphers does not anticipate or render the above underlined sections obvious.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

A. RSA Laboratories, "RSA Security Response to Weaknesses in Key Scheduling Algorithm of RC4", discloses suggestions for improving the key scheduling algorithm by using hash functions rather than adding or concatenating a counter value to the base key.

B. Venkaatesan et al. (US 6,490,354) discloses an method for improving a stream cipher by applying hash functions to the output of the stream.

C. Matthews, Jr. (US 6,549,622) discloses a method for increasing the implementation of the RC4 algorithm.

D. McGrew et al. (US 6,862,354) discloses a method for decrypting encrypted packets of data lost in transmission or received out of order by using a keystream segment arbitrarily located a number of bits ahead of the current state keystream.

E. Duval (US 2002/0037079) discloses a method for reducing the computation load on the system CPU while executing RC4 encryption/decryption operations by using an encryption accelerator.

F. Tuvell (US 2002/0044651) discloses a method for improving the security of cryptographic ciphers by modifying the fixed secret key with a variable non-secret initialization vector.

G. Parker et al. (US 2002/0186839) discloses an apparatus for improving the throughput of the RC4 algorithm by reducing the number of clock cycles needed to perform the encryption/decryption operations.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B. Smithers whose telephone number is (571) 272-3876. The examiner can normally be reached on Monday-Friday (8:00-4:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel L. Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew B Smithers
Primary Examiner
Art Unit 2137